BOLETÍN DE ALERTA

Boletín Nro.: 2023-34
Fecha de publicación: 21/07/2023
Tema: Vulnerabilidad de ejecución remota de código (*RCE*) en el *ssh-agent forwarded* de OpenSSH

Software afectado:

- OpenSSH, versiones 5.5 y previas a 9.3p1.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta al *ssh-agent forwarded* de OpenSSH, que permitiría a un atacante realizar ejecución remota de código (*RCE*). Actualmente para esta vulnerabilidad existe prueba de concepto (*PoC*) publicado.

La vulnerabilidad identificada como CVE-2023-38408 sin severidad ni puntuación asignada aún. Esta vulnerabilidad se debe a una falla de validación segura de rutas de búsqueda en la funcionalidad PKCS#11 del reenvío de conexión del *ssh-agent* de OpenSSH; generalmente utilizado para la automatización de tareas remotas. Esto permitiría a un atacante remoto a través de bibliotecas de proveedores especialmente diseñadas basadas en *sockets* en el sistema de la víctima, obtener el control y realizar ejecución remota de código en el *ssh-agent.*

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante remoto obtener el control y realizar ejecución remota de código en el sistema afectado.

Prevención:

Existen medidas de prevención que se deben tener en cuenta para protegerse de esta vulnerabilidad, las siguientes son:

- Se debe actualizar a OpenSSH 9.3p2 o posterior.
- Configurar OpenSSH para permitir solo proveedores específicos de la funcionalidad PKCS#11.
- Tener cuidado al reenviar el *ssh-agent* a servidores que no son de confianza.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante en la siguiente guía:

- https://www.openssh.com/txt/release-9.3

Adicionalmente, en caso de sospecha de que el sistema fue comprometido se debe seguir los siguientes pasos:

- Cambiar las contraseñas.
- Analizar el sistema en busca de código malicioso.
- Denunciar el ataque ante las autoridades.

Información adicional:

- https://securityonline.info/cve-2023-38408-openssh-remote-code-execution-vulnerability/
- https://blog.qualys.com/vulnerabilities-threat-research/2023/07/19/cve-2023-38408-remote-code-execution-in-opensshs-forwarded-ssh-agent
- https://nvd.nist.gov/vuln/detail/CVE-2023-38408
- https://www.openssh.com/txt/release-9.3